UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

EDNA FRANCHINI and VALERIE SEALS, individually and on behalf of all others similarly situated, *Plaintiffs*, v. ACCU-TIME SYSTEMS, INC., *Defendant*.	21-cv-05075 Hon. Steven C. Seeger

PLAINTIFFS' RESPONSE TO DEFENDANT ACCU-TIME SYSTEMS, INC.'S RENEWED MOTION TO DISMISS

INTRODUCTION

In 2008, and after a unanimous vote, Illinois enacted the Illinois Biometric Privacy Act, 740 ILCS 14/1 et seq. ("BIPA"), to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction" of individuals' biometric data. *Id.* at 14/5(g). BIPA restricts a private entity from collecting or possessing individuals' biometric identifiers or information without following the law's strict but easy-to-follow requirements. Defendant Accu-Time Systems, Inc. ("Defendant" or "ATS") failed to adhere to these requirements and violated BIPA.

Defendant is global provider of biometric hardware and timekeeping services, including software and cloud-based storage. Defendant argues that this Court lacks specific personal jurisdiction over it despite cases directly on point that undermine its position. Plaintiffs' well-plead allegations demonstrate that Defendant collected biometric information in Illinois, uploaded it to the cloud, and then disclosed the information to a third party. In violation of BIPA, Defendant's software "engine" allowed it to collect, store, and disclose at least 14,000 Illinoisians' biometric information. This was not "random" nor "fortuitous": Defendant has earned hundreds of thousands

of dollars in revenue from collecting ***tens of thousands*** of biometric scans ***each month*** in Illinois. The information is collected on biometric devices that Defendant sold to Illinois-based companies and continues to control remotely. Having been sued, Defendant entered into thousands of contracts with Illinois-based workers governing the collection of their biometric data.

Defendant's Motion further mischaracterizes Plaintiffs' factual allegations as meager "conclusions". Instead, Plaintiffs' Complaint gives Defendant "fair notice of what the. . . claim is and the grounds upon which it rests." *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The claims stem from Defendant's continued involvement as the vendor of time management solutions that utilize a biometric reader. Plaintiffs allege that Defendant remains entrenched in the biometric collection and transmission process even after it distributes the equipment.

FACTS

Defendant is a "manufacturer of time and attendance terminals and data collection and storage equipment, systems, and software." Complaint at ¶ 1 (ECF 16-1). It "uses and supplies" a time-tracking system that utilizes a fingerprint to identify employees who clock in and out. *Id.* ¶ 27. Defendant designs and provides "fully-integrated time and attendance production, system, and services to businesses," including the business that directly employed Plaintiffs. *Id.* ¶ 2. *See also* Def. Ex. B, Gladysz Decl., ¶ 4. When utilizing Defendant's time management systems, users are required to scan their biometric identifiers (e.g. fingerprints) as an authentication method. Compl. ¶ 3. Plaintiffs allege that they enrolled in Defendant's biometric system and that their fingerprint data was stored in Defendant's databases and transmitted using Defendant's software. *Id.* ¶¶ 4, 38.

Jurisdictional discovery confirms that personal jurisdiction is appropriate in this case:

- In Illinois, 124,000 employees at any given time use Defendant's timeclocks at work. Approximately 14,000 employees use its biometric scanners. *See* Exhibit 1, Defendant's Fed. R.

Civ. Pro. 30(b)(6) deposition transcript, pp. 7-8, 44.[1] These employees work for the Defendant's 33 Illinois-based customers (of which between 16 and 18 use Defendant's biometric scanners). *Id.* p. 8-10, 15. These figures are for direct Defendant-to-customer sales; and do not account for the Defendant's Illinois sales through its reseller network. *Id.* pp. 12, 14-15.

- Defendant knows its biometric clocks are being used in Illinois because it ships them here and it pays Illinois sales tax. *Id.* p. 12, 37.

- Last year, Defendant deployed 154 active biometric timekeeping clocks in Illinois at its direct customers' locations (not including those sold through re-sellers). *Id.* p. 18. Defendant maintains control over its biometric timeclocks by being able to modify the "workflow" on them which, among other things, means Defendant can modify what appears on the screen in Illinois and to cause the biometric information to transfer. *Id.* pp. 32, 42-43, 45, 82.

- Each time an Illinois-based worker punches in with a fingerprint, the biometric device "captures the image" and that biometric information is stored on the Illinois-based timeclock. *Id.* p. 42-43, 45, 82. Defendant's software/firmware, which is installed on the Illinois-based biometric collection device, causes the employees' biometric information to transfer to Defendant's remote server to confirm an identity match of the worker. *Id.* p. 42, 46. Defendant's software program is the "engine" that drives the transfer of biometric data off the timeclock in Illinois and onto the Defendant's servers. Defendant, through software and/or firmware that it owns, causes the biometric information to transfer to a third-party in Virginia. *Id*. pp. 39, 41, 48. *See also* Exhibit 2, Ecolab Deposition, pp. 31-32, and 81, 83 (noting that "ATS obtained [the biometric information] in the first place" from Ecolab customers, rather than the employer customer).

[1] This figure is from 2021; the number fluctuates based on customer/employee counts. As this figure represents a snapshot of an employee count from late 2021, the total class numbers over 5 years will presumably be more due to employee turnover of the hourly-rate workforce at Defendant client locations. *Id.* p. 10.

- Defendant earns revenue from Illinois by selling and servicing its Illinois-based biometric collection devices. Examples of ongoing revenue Defendant receives include: (1) approximately $25,000 when a customer starts as a set-up fee; (2) $1,500 to $1,600 per device as the cost of the biometric timeclock; (3) between $500 to $2,000 per month for a "ConstantSupport" service contract; (4) and a "hosting" fee of $25 to $30 per device per month. *Id.* pp. 49-52. Extrapolating these ranges ***just*** for the 18 Illinois-based biometric direct customers (as reported ***just*** during the 2021 snapshot discussed above) demonstrates that the Defendant has earned approximately $450,000 for start-ups (18 x $25,000), $234,000 for the devices themselves (156 devices x $1500), about $4,500 *per month* for hosting fees (156 devices x $25 per device), and $25,000 *per month* for ConstantSupport (18 customers x $1,500 per month).

- Part of the service that an Illinois customer pays the Defendant to perform, by contract, is the hosting service that includes the storage of the finger scan information. *See* Exhibit 2, Ecolab Dep., pp. 31-33, 34-35.

- Defendant's revenue figures are from the ~10% of the Defendant's Illinois clients who use the biometric feature (again, only about 14,000 of the 124,000 workers use a biometric device). In other words, it does not include the ~90% (estimate) of Illinois-originated revenue from the Defendant's non-biometric devices. It also does not include the revenue collected from sales done through the Defendant's network of resellers to Illinois customers (*i.e.*, indirect sales).

- To assure the biometric clocks keep working, Defendant sells a "ConstantSupport" subscription service and maintenance package to customers; this service is required for Defendant's Illinois-based customers that utilize biometric collection devices. *Id.* pp. 53-56. As the ContantSupport name implies, this service monitors its customers through continuous

"pinging" of the biometric collection device's health and activity. It supplies diagnostic tools, allows for upgrades, customer support, and repairs on the devices. *Id.* pp. 53, 57-58.

- Defendant provides Illinois-based customers service and support and has a "Devops" team that receives alerts to monitor that its systems are functioning correctly. *Id.* pp. 54-55, 57.

- Post-sale, Defendant provides an equipment maintenance plan for the biometric collection timeclocks. If one breaks, Defendant overnights a new one to its customer along with a prepaid package to return the broken device. *Id.* p. 52. Defendant provides a warranty on this Illinois-based equipment. *Id.* p. 66. Once the warranty service runs out, Defendant invoices its Illinois-based customers for repair work it performs. *Id.* p. 67. When equipment is returned from Illinois, Defendant assumes the responsibility of deleting the Illinois workers' biometric data off the device before placing it into a future use pool. *Id.* p. 84.

- Defendant ultimately enacted a biometric policy specifically (and only) for the thousands of Illinois-based employees who utilize its equipment. *Id.* p. 21.[2] It provided this policy to each of its Illinois-based customers, including Ecolab where the Plaintiffs worked. *Id.* p. 24.

- Defendant entered into approximately 14,000 agreements with Illinois-based workers regarding the collection of their biometric information.[3] Defendant ultimately modified its Illinois-based biometric timeclocks so that when a worker is enrolled, they need to enter into an agreement regarding the collection of their biometric information. *Id.* pp. 27-28, 31. Defendant now considers itself contractually bound to manage biometric information in compliance with this Illinois-

[2] While the Defendant's counsel refused to allow the witness answer when this was done, Plaintiffs believe that discovery will demonstrate that this was an ineffective after-the-fact effort to comply with BIPA—year after Defendant became aware of the biometric law and only after it had been sued. *See e.g., Mora v. J&M Plating, Inc.* 2022 Ill App (2d) 210692 (late BIPA policy does not comply with statute).

[3] Again, the Defendant's counsel refused to allow the witness to answer when this was done.

specific agreement it entered into with thousands of Illinoisians and it maintains records of the approximately 14,000 employees who signed the agreement. *Id.* pp. 35-37; 78.

- Defendant trains its Illinois-based customers on how to correctly have their employees scan their fingerprints and can provide its Illinois-based customers with reports such as identifying those workers who are enrolled in its biometric collection devices. *Id*. pp. 59, 64.

- When a customer requests that Defendant install the biometric collection devices, Defendant contracts with a third-party to put them at the customer location and Defendant coordinates for the installation in Illinois by scheduling delivery, a technician, and overseeing project management. *Id.* pp. 60-61, 64.

- Defendant maintained an office in Oak Brook, Illinois through 2017 because it rented an office for a now-retired vice president/salesperson who worked here who helped "nurture" customer relationships. *Id.* pp. 69-70.[4] Defendant also attended tradeshows in Illinois and obtains leads and inquiries from customers, some of whom are based in Illinois. *Id.* pp. 74-75.

- Defendant is registered to do business in Illinois. *Id.* pp. 75; Exhibit 3, *Ill. Sec of State*.

LEGAL STANDARD

First, when ruling on a Rule 12(b)(2) motion to dismiss based on the parties' submission of written materials without an evidentiary hearing, such as here, the Plaintiffs need only make a *prima facie* showing of personal jurisdiction. *Matlin v. Spin Master Corp.*, 921 F.3d 701, 705 (7th Cir. 2019). As such, any factual disputes that may arise between the parties' written materials must be resolved in Plaintiffs' favor. *RAR, Inc. v. Turner Diesel, Ltd.*, 107 F.3d 1272, 1275 (7th Cir. 1997). Further, when considering a Rule 12(b)(2) motion to dismiss, the court must accept all undisputed, well-pleaded facts alleged in the complaint as true. *Mutnick v. Clearview Al, Inc.*, No.

[4] Defendant refused to answer why it rented office in Illinois. *Id.* p. 71

20-c-0512, 2020 WL 4676667, at *1 (N.D. Ill. Aug. 12, 2020). A complaint will survive a Rule 12(b)(6) motion if it "contain[s] sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

ARGUMENT

I. THIS COURT HAS JURISDICTION OVER DEFENDANT

Jurisdiction is general or specific, depending upon defendant's contacts with the forum state. *uBID, Inc. v. GoDaddy Grp., Inc.*, 623 F.3d 421, 425 (7th Cir. 2010). Specific jurisdiction is determined by "the relationship among the defendant, the forum, and the litigation." *Walden v. Fiore*, 571 U.S. 277 (2014). To establish specific personal jurisdiction over an out-of-state defendant, Plaintiffs need only show that (1) Defendant "purposefully availed [itself] of the privilege of conducting business" in Illinois (2) Plaintiffs' suit arises out of or relates to Defendant's contacts with the forum state, and (3) it would not offend "traditional notions of fair play and substantial justice" for Defendant to litigate in the forum state. *Greene v. Karpeles*, No. 12-c-1473, 2019 WL 1125796, at *5 (N.D. Ill. Mar. 12, 2019).

The fundamental inquiry is: "is it fair and reasonable to call the defendant into the state's courts to answer the plaintiff's claim?" *uBID*, 623 F.3d at 426 (7th Cir. 2010). This is a broad standard, and the Supreme Court has found that sufficient minimum contacts may take many forms. *Id.* Sufficient minimum contacts include a defendant "exploiting a market in the forum State[,] entering a contractual relationship entered there," and shipping products to the forum state. *Ford Motor Co. v. Montana Eighth Judicial District Court*, 141 S. Ct. 1017, 1025 (2021). "So long as it creates a substantial connection with the forum, even a single act can support jurisdiction." *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 n. 18 (1985). *See also uBID*, 623 F.3d at 425 (finding sufficient minimum contacts because a portion of the offending domains were registered

to Illinois addresses and other evidence supported that GoDaddy exploited the Illinois market).

A. This Court Has Personal Jurisdiction Over Defendant Because It Purposefully Directed Its Biometric Timekeeping Services Towards Illinois, and Plaintiffs' Claims Arise Out of Defendant's Illinois-Directed Activities.

Defendant's direct and knowing provisioning of products to Illinois-resident businesses is sufficient to establish purposeful availment of the Illinois market. *See, e.g., uBID*, 623 F.3d at 429 ("GoDaddy purposefully availed itself of the Illinois market for its services through its deliberate and continuous exploitation of that market"); *Illinois v. Hemi Grp. LLC*, 622 F.3d 754, 758 (7th Cir. 2010) (finding the defendant purposefully availed itself of doing business in Illinois because it "knowingly . . . d[id] business with Illinois residents"). "When a corporation purposefully avails itself of the privilege of conducting activities within the forum State, it has clear notice that it is subject to suit there." *Asahi Metal Indus. Co., Ltd. v. Superior Court*, 480 U.S. 102, 110 (1987). *See also Burger King*, 471 U.S. at 474-75 (defendant did not physically enter the forum but "purposefully avail[ed]" itself of the benefit and protection of the forum state's laws by entering into long term business franchise contract with a resident of the forum).

Significantly, here the Defendant's contacts with Illinois (sales of biometric collection devices and the transferring Plaintiffs' biometrics to out of state servers) is directly related to the claims at issue; this alone supports personal jurisdiction. *See Kukovec v. Estee Lauder Companies, Inc.*, 22 CV 1988, 2022 WL 16744196, at *4 (N.D. Ill. Nov. 7, 2022)(in BIPA case, personal jurisdiction established where an Internet page collected biometric information in Illinois--even though it was through a geographic neutral Internet site--because the contact was tied directly to specific claim); *Trio v. Turing Video, Inc.*, 1:21-CV-04409, 2022 WL 4466050, at *5 (N.D. Ill. Sept. 26, 2022)(even though no physical presence, where customers purchased machines that collected biometrics, personal jurisdiction established); *Crumpton v. Haemonetics Corp.*, 595 F. Supp. 3d 687, 697 (N.D. Ill. 2022)(in BIPA case, finding personal jurisdiction where defendant

"deliberately entered into contractual and business arrangements to ensure that its software collected data in Illinois and …hosted Illinois resident's data on its servers".)

King v. PeopleNet Corp., No. 21-cv-2774, 2021 WL 5006692 (N.D. Ill. Oct. 28, 2021) is directly on point. In *PeopleNet*, the court found that it had specific personal jurisdiction over an out-of-state defendant that supplied its Illinois-based clients with biometric scanners. *Id.* at *1. As here, the scanners collected employee data before transmitting the data to the defendant's cloud-based storage. *Id.* at *2 ("The devices captured employee data and transmitted it to defendant's cloud-based time and attendance systems, hosted on PeopleNet's servers."). The defendant argued that it was merely a vendor for its Illinois-based clients and that any contacts it had with Illinois were attenuated. *Id*. at *6. This Court rejected that argument, finding that the defendant directly did business with the plaintiff's Illinois employer and other Illinois-resident businesses. *Id*. Further, the court noted that the defendant shipping devices and providing services to its Illinois clients, and having machines collect biometric information in Illinois, was sufficient to show that defendant exploited the Illinois market. *Id*.

In another similar case, *Fisher v. HP Property Management, LLC*, 2021 IL App (1st) 201372, the plaintiff sued both the employer and KEYper, a company that manufactures a biometric scanner. KEYper, an out-of-state entity, argued that the court lacked personal jurisdiction because its in-state customer's activities could not be attributed to it. The Illinois Appellate Court disagreed because (as with the Defendant here) KEYper "agreed to provide ongoing data management services, including hosting, storing, transmitting, and processing the Illinois user biometric data collected by the KEYper device." *Id.* at ¶ 30. The court pointed out that even though the plaintiff in that case could *not* show that there were thousands of Illinois users (something Defendant here has admitted), it provided "an Illinois company, with a device that

repeatedly scanned employees' fingerprints in Illinois and continually serviced Illinois employees' data for future use," thereby meeting the "minimum contacts" requirement. *Id.* at ¶ 42.

Therefore, there is specific personal jurisdiction over Defendant in Illinois. *See, Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1105 (N.D. Ill. 2015) (personal jurisdiction against biometric collector exists because BIPA "is an Illinois statute and [the case] stems out of … contact with Illinois residents [and] Illinois [has] a strong interest in adjudicating the matter locally").

B. It is Reasonable to Exercise Jurisdiction over the Defendant.

The Court must examine whether exercising jurisdiction would be reasonable and not offend "notions of fair play and substantial justice." *Burger King*, 471 U.S. at 476-77. As found in *Tavel v. Riddle*, No. 20-cv-6805, 2021 WL 1121120, at *4 (N.D. Ill. Mar. 24, 2021), "a threshold showing of minimum contacts,…is generally only defeated if the defendant presents a compelling case that the presence of some other considerations would render jurisdiction unreasonable." *Id.* (internal quotations and citations omitted). Defendant presents zero considerations which would render jurisdiction unreasonable, and its Motion must therefore be denied. *See Harding v. Cordis Corp.*, 2021 IL App (1st) 210032, ¶ 48 (only contesting minimum contacts, without putting forth evidence that would be unreasonable to litigate in Illinois, warrants denial of challenge to personal jurisdiction when Illinois residents impacted by product at issue).

Plaintiffs make a *prima facie* showing of specific personal jurisdiction over Defendant because Defendant purposefully availed itself of conducting business in Illinois. Defendant is registered to do business in Illinois and provides biometric timekeeping devices to approximately 16 Illinois-based employers, including Plaintiffs' employer, Ecolab, Inc., linking approximately 154 devices located in Illinois to Defendant's servers. *See* Exhibit 1, ATS Dep., pp. 8-10, 15. Further, Defendant operates a warranty program for its biometric timekeeping devices, meaning that its customers, including its Illinois clients, ship defective devices to Defendant for replacement

and, in return, receive new devices directly shipped from Defendant. *Id.* pp. 66-67.

What's more, Defendant enacted a policy that specifically targets the Illinois-resident employers it conducts business with regarding Illinois employees' use of its biometric timekeeping devices, showing that Defendant's conduct and connection with Illinois is such that it could reasonably anticipate being sued in Illinois. Defendant adapted its services to its Illinois customers; its relationship with its customers developed out of its activities in Illinois. Therefore, it would not be unreasonable to expect Defendant to defend the BIPA claims here.

The cases relied upon by Defendant are distinguishable because none involve a situation where a company entered into contracts (let alone thousands of contracts) with Illinois workers, directly had its equipment commit the offending act of biometric collection in Illinois, continued to control and collect the biometric data in Illinois (through its servers and cloud-based storage), and even made Illinois-specific (and no other state) biometric policies. *See e.g.*, *Bray v. Lathem Time Co.*, 2020 WL 1492742, at *4 (C.D. Ill. Mar. 27, 2020)(timeclock manufacturer who had no contacts whatsoever in Illinois and, in fact, sold the timeclock in question to an Arkansas-based customer who ended up moving the biometric collecting device into Illinois).

Perhaps the best that can be said for Defendant is that it did not actually send its employees directly into Illinois to collect biometric information (that would be impossible because only an electronic device, not a human, has the precision necessary to collect biometrics). But "cases make clear…that [physical] presence is not necessary for a defendant to have sufficient minimum contacts with a state." *Curry v. Revolution Labs., LLC*, 949 F.3d 385, 389 (7th Cir. 2020) (rejecting argument that jurisdiction requires specifically targeting a local market when the defendant shipped products here and sent an email thanking purchasers).

In actuality, not only *should* Defendant "reasonably anticipate being haled into court"[5] in Illinois, it *did* anticipate being sued here by the time this lawsuit was filed. Defendant *was* sued in 2019 for allegedly violating BIPA. *See Shelby-Williams v. Accu-Time Systems, Inc. et al*, 2019 CH 14363 (Cook County, Illinois) (Exhibit 5). Thereafter, Defendant enacted an Illinois-specific biometric policy that was applicable only to Illinois customers. Defendant rolled out a contract to appear on the screen of its Illinois-based biometric collection devices.[6] So, by the time this lawsuit was filed, Defendant clearly anticipated another case being filed and was making efforts to comply with the law, albeit too late.

Accordingly, because Plaintiffs make a *prima facie* showing of personal jurisdiction and because Defendant failed to rebut any of Plaintiffs' well-pleaded allegations, this Court should deny Defendant's Motion to Dismiss under Rule 12(b)(2).

II. PLAINTIFFS' BIPA ALLEGATIONS ARE SUFFICIENTLY PLEAD

Defendant argues that the Complaint is insufficiently plead on two grounds. First, Defendant makes a blanket argument that Plaintiffs cannot state a claim under either Sections 15(a), (c), or (d) of BIPA because they have not alleged sufficient facts to establish Defendant's "possession" of biometric data. Second, as to Plaintiff's Section 15(b) claim, Defendant argues that Plaintiffs did not allege sufficient facts to establish that Defendant "collects" biometric data. Defendant argues that under these subsections of BIPA, either a showing of "possession" or "collection" is material and without the required allegation Plaintiffs cannot state a claim.

---

[5] *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 474, 105 S. Ct. 2174, 2183 (1985).

[6] In violation of this Court's Standing Order regarding depositions, the Defendant refused to allow basic questions that are clearly relevant such as whether the Defendant anticipated being sued in Illinois. *See. e.g.* pp. 32-33. Plaintiffs believe discovery will show that the Defendant knew years earlier about potential liability biometric liability and waited until after it was first sued to do anything about it.

Under Rule 8, a plaintiff need only provide "a short and plain statement of the claim showing that the pleader is entitled to relief, in order to give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555). "Specific facts are not necessary; the statement need only give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.'" *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009) (quoting *Erickson v. Pardus*, 551 U.S. 89, 93 (2007)).

As an initial matter, Plaintiffs need not separately establish their claims under BIPA's different subsections as they have alleged a single count complaint and a "motion to dismiss under Rule 12(b)(6) doesn't permit piecemeal dismissals of parts of claims[.]" *BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015). The law provides that "[a] prevailing party may recover" a range of remedies in Section 20, including liquidated damages for negligent and reckless/intentional violations. 740 ILCS 14/20(1)-(2).

Plaintiffs plead in detail that Defendant collected, stored, and disseminated their biometric. For example, Plaintiffs allege that:

- "When individuals scan their fingerprint…in a Defendant biometric time tracking system as a means of authentication, their biometric information and biometric data is transmitted to a Defendant database." Compl. ¶¶ 4, 5.

- "Defendant's equipment required Plaintiffs to scan their fingerprint into a Defendant biometric system so that the data could be uses it as an authentication method to track time. Defendant subsequently stored Plaintiffs' fingerprint data in its databases and transmitted the data using Defendant's software." *Id.* ¶ 38.

- The biometric "data is broadcast through Defendant's software and web-based data collection and storage system" *Id.* ¶ 6.

- "When individuals use Defendant's biometric systems, they are required to have their fingerprints captured and stored to enroll them in Defendant's equipment, systems, and database(s);" *Id.* ¶ 26.

- "Defendant … discloses…fingerprint data to…one… third-party vendor;" *Id.* ¶ 28.

- "Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiffs' biometric identifiers;" *Id.* ¶ 63, 66. "Defendant continued to collect, store, use, and disseminate Illinois employees' biometric data". *Id.* ¶ 25.

Allegations that Defendant collected and possessed the biometric information on its equipment and servers and broadcast the biometric information through its software (including by disclosing it to an out-of-state vendor) must be taken as true. Rule 8 and the *Twombly/Iqbal* standard do not require more.

Biometric identifiers were collected on Defendant's biometric readers, and "transmitted to a Defendant" database, "broadcast through Defendant's software and web-based data collection and storage system." *Id.* ¶¶ 5-6. These allegations meet Rule 8 pleading requirements. *See, Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 784 (N.D. Ill. 2020)(similar BIPA allegations sufficient to state claim against timekeeping vendor); *Ronquillo v. Doctor's Associates, LLC*, 597 F. Supp. 3d 1227, 1231–32 (N.D. Ill. 2022)(BIPA allegations that defendant's technology stores and compares biometric data sufficient to allege collection).

The *PeopleNet* case previously discussed on the issue of jurisdiction is instructive here as well. In *PeopleNet*, the court denied a motion to dismiss a complaint with similar allegations. The court reasoned "the complaint alleges that defendant did more than possess King's biometric information: it says that PeopleNet *collected and obtained* it. *I accept that factual allegation as true,* and it's reasonable to infer that PeopleNet . . . was doing the capturing and obtaining of King's biometric information" because plaintiff alleged the collection occurred through PeopleNet's time clocks. *PeopleNet.* No. 21-cv-2774 at *19 (N.D. Ill. Oct. 28, 2021) (emphasis added, internal citation omitted). Additionally, in the BIPA case *Neals v. ParTech*, the plaintiff alleged that defendant developed a cloud-based point of sale system, and that the plaintiff used the biometric finger scanner when working for a restaurant that used the system. 419 F.Supp.3d 1088,

at 1090. The defendant in *ParTech* made a similar argument to Defendant here—that the plaintiff must allege the details of collection. The court found, "Plaintiff presents 'a story that holds together'" by alleging that the defendant collected information through its customer's use of the biometric system. *Id.* In *ParTech*, the plaintiff did not specify where she worked. Yet, the court considered Defendant's violations separate from conduct of its clients. *See also, Hazlitt v. Apple Inc.*, 543 F.Supp.3d 643 (S.D. Ill. June 14, 2021)("possession" under BIPA need not include exclusive control, relying on allegation that defendant used its software to gather the data and store it in databases); *Wordlaw v. Enter. Leasing Co. of Chi., LLC*, 2020 WL 7490414, at *4 (N.D. Ill. Dec. 21, 2020) ("The data needed to be possessed to connect an employee to the hours worked—the purpose of the timekeeping system implies possession."). Here, Plaintiffs allege the same. Plaintiffs sufficiently allege possession of biometric data.

A. Alternatively, Defendant Admits A Plausible BIPA Violation.

The Defendant's own witness explained precisely how the collection and possession occurs. These facts may be considered in this Response because a "party opposing a Rule 12(b)(6) motion may submit materials outside the pleadings to illustrate the facts the party expects to be able to prove". *Geinosky v. City of Chicago*, 675 F.3d 743, 745, fn1 (7th Cir. 2012). Defendant admits that its biometric device "captures the image" and stores it on the timeclock (Ex. 1, pp. 42-43, 45, 82) and then its software/firmware (the "engine") causes the biometric information to transfer to a remote server to confirm an identity match. *Id.* pp. 39, 41-42, 46, 48. This is (at least) a plausible BIPA violation.

CONCLUSION

Therefore, Plaintiffs respectfully request that this Court deny Defendant's Motion to Dismiss.

Dated: March 16, 2023

Respectfully submitted,

/s/David Fish
One of Plaintiffs' Attorneys

David Fish (dfish@fishlawfirm.com)
Mara Baltabols (mara@fishlawfirm.com)
FISH POTTER BOLAÑOS, P.C.
200 East Fifth Avenue, Suite 115
Naperville, Illinois 60563
Tel: 312.861.1800

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that on March 16, 2023, the foregoing was filed electronically with the Clerk of Court using the ECF system, which sent notification of such filing to all counsel of record.

/s/ David Fish
One of Plaintiffs' Attorneys